CHAPTER 7
SECURITY CONSIDERATIONS

7-1. Environmental threats

SCADA equipment installed in C4ISR facilities must be of such design or otherwise protected to withstand seismic effects as well as shock (ground motion) and overpressure effects of weapons. A detailed dynamic analysis should be made of the supporting structure(s) of the equipment enclosures to evaluate the magnitude of motion and acceleration established at the mounting points for each piece of SCADA equipment. Where accelerations exceed the allowable limits of equipment available, the equipment should be mounted on shock isolation platforms.

a. SCADA equipment should be protected from the effects of dust, dirt, water, corrosive agents, other fluids and contamination by appropriate location within the facility or by specifying enclosures appropriate for the environment. Care should be taken that installation methods and conduit and tubing penetrations do not compromise enclosure integrity.

b. Central computer or control rooms should be provided with dry agent fire protection systems or double-interlocked pre-action sprinkler systems using cross-zoned detection, to minimize the threat of accidental water discharge onto unprotected equipment.

c. Sensors, actuators, controllers, HMI, UPS and other SCADA equipment located throughout the facility should utilize enclosures with a minimum environmental protection level of IP66 per EN 60529 or Type 4 per NEMA 250. Where thermal management issues or other equipment requirements prevent use of such enclosures, alternate means should be provided to protect the equipment from environmental contaminants.

d. Facility design must ensure that any facility chemical, biological, radiological, nuclear or explosive (CBRNE) protection warning, alert, or protection systems also protect SCADA systems and utility equipment areas if the mission requires the facility to remain operational in a CBRNE environment. Appropriate coordination and systems integration must occur between SCADA and CBRNE protection systems so that appropriate facility environmental conditions are maintained if the facility experiences a CBRNE attack or incident.

7-2. Electronic threats

Electronic threats to SCADA systems include voltage transients, radio-frequency (RF) interference (RFI), RF weapons, ground potential difference and electromagnetic pulse (EMP). These threats can all be largely mitigated by proper design of the systems

a. SCADA controllers and field devices are vulnerable to voltage transients coupled through the facility power system from atmospheric (thunderstorm and lightning) effects, transmission and distribution system switching events, and switching of capacitors or inductive loads within the facility. Transient voltage surge suppression (TVSS) should be provided on the power supply circuits to all SCADA equipment and TVSS or optical isolation should be provided on all metallic control and communication circuits transiting between buildings. To avoid the effects of voltage transients, fiber optic cable should be used for all circuits entering or leaving a facility. Fiber media are available for most network applications at the supervisory and control levels (see paragraph 4-1). Field devices typically require metallic conduc-

tors, and where these must be run outside or between facilities, they should be provided with TVSS where they cross the facility perimeter.

(1) TVSS should be specified to comply with the testing requirements of ANSI C62.34 and should be installed in accordance with IEEE 1100. Selection of TVSS locations and connections should consider that it is most effective when connected directly to the terminals of the device to be protected and provided with a direct low-impedance path to the facility ground system. Incorrect installation methods can readily render TVSS protection ineffective. Protected and unprotected circuits should be physically segregated to avoid capacitive and inductive coupling that may bypass the TVSS. See figure 7-1 for an example of correct TVSS installation.

(2) Network surge protectors should be provided at all device connections, between the equipment port and the tap.

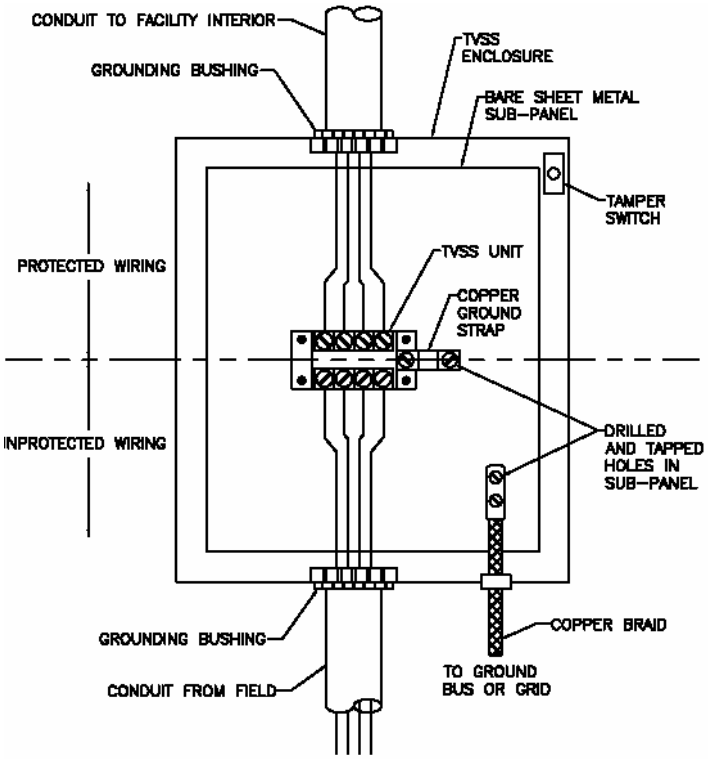

Figure 7-1. Signal level TVSS installation

b. C4ISR facilities often contain powerful radio frequency sources which may interfere with control system operation if coupled into control circuits. Other ambient sources of RFI may also exist including commercial signals, electronic counter measures (ECM), and radiated RFI from other equipment within the facility. Design and operation of SCADA systems should address measures to protect against RFI, including:

(1) Use of shielded twisted pair or twisted triple conductors for low-level signals.

(2) Installation of SCADA wiring in continuous metallic conduit systems.

(3) Use of metallic controller enclosures with RFI-gasketed doors.

(4) RFI-shielded control rooms and computer rooms.

(5) Maintenance practices that maintain the integrity of enclosures.

c. Effective shielding to limit RFI to within the required limits for C4ISR facilities is dependent upon the grounding and bonding practices required to provide a unified facility ground. The grounding practices for the earth electrode system, the building structure, the lightning protection system, the power system, and the signal reference system must be integrated to achieve a unified ground system. The particular grounding practices for each of these subsystems are illustrated in MIL-HDBK-419A, Grounding, Bonding, and Shielding for Electronic Equipment and Facilities. Additionally, specifications and installation designs for new equipment should include requirements to assure electromagnetic compatibility (EMC) between the equipment and the operating environment. These requirements should serve to minimize the susceptibility of the new equipment to EMI that may be present in the operating environment as well as to limit radiated emissions by the equipment to the environment and to existing equipment.

(1) Ground potential differences within a facility that may affect SCADA systems are mitigated by proper connection of equipment to the unified grounding system that is required to be provided for all C4ISR facilities. This system ties the electrical service, lightning protection, and all other facility grounds together into a single low-impedance ground grid. Additional grounding requirements for C4ISR facilities may be found in TM 5-690, Grounding and Bonding in C4ISR facilities.

(2) Each electrical room within the C4ISR facility which contains electrical equipment should be provided with a ground bus, connected to the unified ground system. SCADA equipment enclosures and internal ground buses should be connected directly to this ground bus, and should not rely solely on an equipment grounding conductor installed with the power supply circuit.

(3) All exterior metallic components which penetrate the building, such as metal piping, conduits, and ducts, should be grounded at the point of penetration. All conductive SCADA circuits entering the facility from outside should be provided with TVSS, effectively grounded to the ground grid at the point of entry.

(4) Low-voltage shielded cables must be installed to avoid ground loops, which can induce interfering currents on the signal common conductor. Unless otherwise dictated by the equipment manufacturer, cable shields should be grounded at the controller end only, with the instrument end left floating and insulated.

(5) On large multi-facility sites potential differences between the different facilities' ground systems caused by atmospheric electrical activity and electrical system faults can not be prevented, in spite of their common connection through the facility primary electrical distribution grounding system. SCADA circuits installed between facilities on these sites should always utilize fiber optic cables or optical signal isolation at the facility perimeter.

d. EMP protection requires magnetically continuous ferrous shielding which is not provided by the enclosures of typical SCADA sensors, controllers and actuators. For this reason, all electronic SCADA components must be assumed vulnerable to EMP and must be protected by location, external shielding, or replacement with pneumatic components.

(1) Whenever possible, all SCADA components should be located inside the C4ISR HEMP shield. Components that must be located outside the shield, such as sensors at an external fuel storage tank, may

be provided with a local HEMP-shielded enclosure and circuits routed back to the facility within a shielded conduit system or using pneumatic lines or optical fiber cable.

(2) EMP protection for non-conductive penetrations of the facility shield such as pneumatic tubing and fiber optic bundles uses the principle of "waveguide below cutoff" in which the lines penetrate the facility shield through a high aspect-ratio cylinder or waveguide. The waveguide must be made of a conductive material and must be continuously welded or soldered to the primary EMP shield so that current flowing on the waveguide can be discharged to the primary EMP shield.

(3) The maximum inside diameter of a penetration must be 4 inches or less to achieve a cutoff frequency of 1.47 GHz for a rectangular penetration and 1.73 GHz for a cylindrical penetration. The unbroken length of conducting material adjacent to the penetration must be a minimum of five times the diameter of the conducting material (i.e., pipe, duct) to attenuate by at least 100 dB at the required frequencies.

(4) The wave guide filter will be specified in terms of the attenuation over a specified range of frequencies in accordance with TM 5-858-5, Designing Facilities to Resist Nuclear Weapons Effects: Air Entrainment, Fasteners, Penetration Protection, Hydraulic Surge Protection Devices, and EMP Protective Devices.

e. Equipment located in electrical substations or other areas where electrical systems over 600V exist may be subject to particularly harsh transient voltage and transient electrical field conditions associated with power system faults, lightning strikes, and switching surges. This equipment should be qualified to the industry standards applicable to the withstand capability of protective relays, ANSI C37.90.1, C37.90.2 and C37.90.3, which apply to surge voltage, radiated EMI and ESD, respectively. Testing has shown that both STP and coaxial network communications circuits are subject to communications errors in high transient electric field conditions. For this reason, all network communication within the substation environment should be over fiber optic circuits. Even with a fiber communication circuit, the network equipment connected to the fiber may be susceptible to radiated fields or to conducted interference at the power supply. This equipment should be qualified to IEEE 1613, which requires automatic recovery from transient-induced communications disruptions with no false operation and no human intervention.

f. Portable RF weapons of van size down to brief-case size are now commercially available. Many of the above factors will also provide varying levels of protection against this emerging threat. For example, a HEMP shield should provide protections from RF Weapons external to the shield. However, it will provide no protection from an RF Weapon inside the shield. Thus, a critical aspect of protection from this threat is ensuring physical security protection plans, measures, and procedures recognize this threat and mitigate it. Examples of this are to insure that facility guards or security personnel are trained on this threat, are able to recognize RF Weapons, and that procedures are instituted for random or mandatory checks of all items entering the facility.

7-3. Physical security

In general, SCADA system equipment should be located inside secured areas having the same degree of security deemed appropriate for the supported systems. However, the electronic nature of these systems provides opportunities for compromise from both inside and outside the secured area that must be addressed.

a. HMI devices for controllers that provide access to the entire SCADA system shall use password-protected screen access with multiple levels of access control, and automatic logout routines with short

time settings. Password policies for screen savers shall be in compliance with established DoD policies (CJCSI 6510.01D).

b. Equipment enclosures and pull and junction boxes should be kept locked or secured with tamper-resistant hardware. Doors and covers should be provided with tamper switches or other means of detecting attempted intrusion, connected to the site security system. Tamper detection devices should be designed to detect the initial stages of access such as removal of fasteners, unlatching of doors, etc.

c. Raceways and enclosures for SCADA circuits external to the secured area should be designed to resist entry by unauthorized persons. Access to field wiring circuit conductors can potentially provide "back-door" entry to controllers for damaging over-voltages or transients. Outside raceways should consist of rigid steel conduits with threaded and welded joints and cast junction boxes with threaded hubs and tamper proof covers.

d. Conduits exiting the secured area should also be sealed to prevent them from being used to introduce hazardous or damaging gases or fluids into enclosures within the secured area.

7-4. Communication and information networks

Connections from SCADA systems to networks extending beyond the C4ISR facility or between facilities on a common site introduce the threat of attacks.

a. These attacks are of several types:

(1) Unauthorized user access (hacking).

(2) Eavesdropping; recording of transmitted data.

(3) Data interception, alteration, re-transmission.

(4) Replay of intercepted and recorded data.

(5) Denial of Service; flooding the network with traffic.

b. The best defense against these threats is to entirely avoid network connections with other networks within or external to the facility. If they must be used, data encryption techniques should be applied to all network traffic. The following additional means of enhancing security should also be considered:

(1) Physically disconnect when not in use; applicable to dial-up connections for vendor service.

(2) Use fiber optic media which cannot be tapped or intercepted without loss of signal at the receiving end.

(3) One-way traffic; alarm and status transmission only with no control permitted.

7-5. Software management and documentation

With the modern complexity and exposure to intentional software damage that can occur in modern industrial controls systems, it is a good practice to implement a Software Management and Documentation System (SMDS).

a. A SMDS system is software which resides on a dedicated computer on the plant network that monitors all activities of the control system. Such a system should be required for the control system in an important and complex military facility. It allows the facility administrator to do the following:

(1) Control who may use any SCADA application software and what actions can be performed

(2) Maintain a system-wide repository for historical storage of the application configuration files

(3) Identify exactly who has modified a control system configuration or application parameter, what they changed, where they changed it from, and when the change was made

(4) Assure that the control system configuration thought to be running the facility actually is

(5) Support application restoration following a catastrophic event

(6) Generate views into the Software Management System for more detailed analysis of configuration changes

b. Software Management and Documentation systems are available now from the major suppliers of industrial control systems. Having such a system provides the following additional benefits:

(1) Avoids maintaining incorrect or incompatible software versions

(2) Assures that there are not multiple versions of software on file

(3) Prevents multiple users from causing a conflict somewhere on the system

(4) Prevents legitimate changes from being reversed or overwritten

(5) Supports the availability of the system at its maximum

c. Among the specific software that such a system would secure are:

(1) PLC programs

(2) HMI screens

(3) SCADA configurations

(4) CAD drawings

(5) Standard Operating Procedures (SOP’s)

(6) Network Configurations